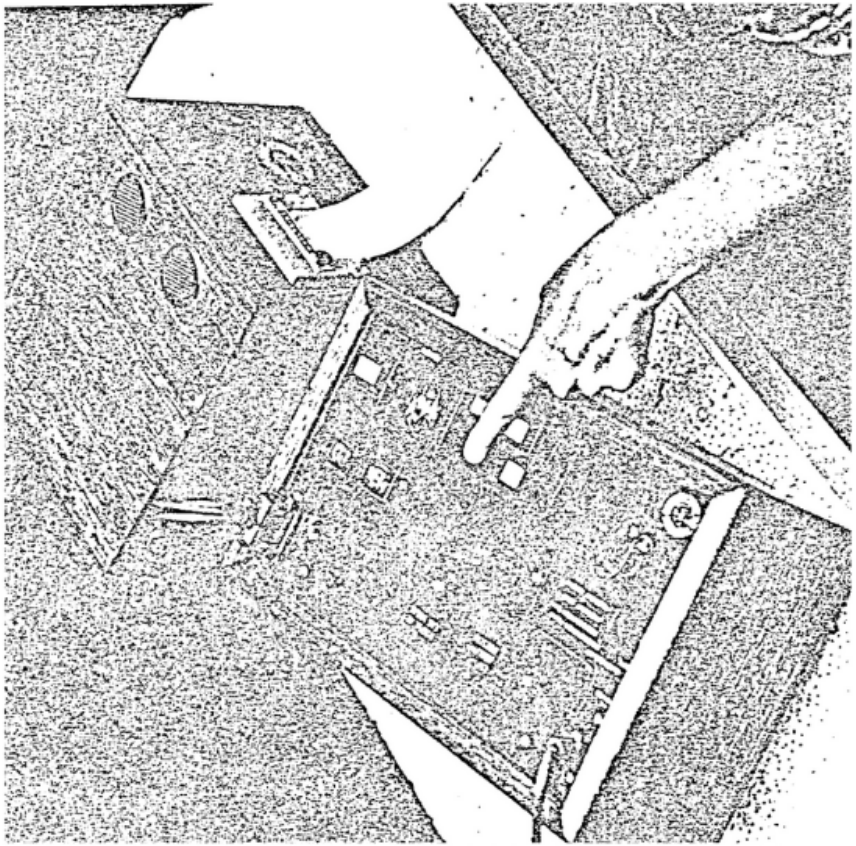
TOP SECRET -

* ENCRYPTION/DECRYPTION
  Hardware encryption according to Federally app
  DES standards. Meets Government and Industry s

* INFINITE ENCRYPTION
  Unlimited encryption upon encryption (with sa
  Keys) for additional data security.



STAT

2. Part-time administrative assistant entered on duty 18 March, in time for PC training. Her pr experience with Wang and other PC systems has given her an unf advantage in becoming "Chief Hacker" on the new IBM system.

Cyber supercomputers in Munich and Hannover have also been accessed by hackers,

The Teletypist

A Periodical Newsletter

Issue 1 Vol.1 $2.00

This work is dedicated to the giants whose shoulders we all stand upon.

Edited by: Sister Eliza Concordia

For The Benefit Of The Reader;

Please maintain the confidentiality of the records within this compendium!

It is of the utmost importance that the contents of this collection remain in the hands of trustworthy individuals, particularly as the sourcing of the information contained within is of a sensitive nature.

I have directed that my staff produce a report with the cleanest, most informative product as is possible. What you are about to read is a collection of government related insight on these issues of community interest.

Whenever possible, we use original communications between government officers & representatives of our sisterhood to preserve the historic value of our research into how the United States Government has seen & dealt with so-called "hacks" & "hackers" over the years.

We have painstakingly collected & compounded decades worth of governmental data into a digested anecdotes both for your education, & for your amusement. This newsletter will be published as new information becomes available to us, and offered to you all at as minimal cost as possible to cover the costs of printing.

Through these documents, you will be given a look beyond the veil of previously classified government information. Through these documents, you, the reader, will see a vision of the evolution of electronic interference, & the pursuit of curiosity through the eyes of the government.

We hope that you will appreciate what we have created, & that these stories will enrich your understanding of both our past, & perhaps even our future.

With Greatest Respect & Gratitude,

Mama Agnes Driscoll

Agnes Driscoll

This Page Intentionally Left Blank

OFFICE OF INTERNAL ASSET RECOVERY

////////////////////////////////////
FOR OFFICIAL USE ONLY
SPECIAL RELEASE//SOCA
////////////////////////////////////

APPROVED BY: DAULTON, JACK

DRAFTED BY: Teletypist

TITLE: "THE HACK THAT NEVER WAS" aka;
ANTISEC,
INTRUSION - INFO SYSTEMS
CONSPIRACY

CASE ID #: A224-AT-98965

KEY JUDGEMENTS:

Φ A SERIES OF ANONYMOUS HACKS IN 2011 IMPACTED LOCAL LAW ENFORCEMENT IN A NUMBER OF US DISTRICTS

Φ THESE HACKS REFERRED TO BY ANONYMOUS GROUP AS "SHOOTING SHERIFFS SATURDAY"

Φ WRITER JUDGES WITH HIGH CONFIDENCE THAT ANONYMOUS GROUP WAS SUCCESSFUL IN EXFILTRATING 10GB OF DATA FROM NUMEROUS US LOCAL LAW ENFORCEMENT OFFICES

IN MID-2011, A ANONYMOUS ADJACENT GROUP KNOWN AS 'ANTISEC' POSTED A 10GB CACHE OF FILES PURPORTED TO BE STOLEN FROM 70 LOCAL SHERRIFF'S DEPARTMENTS, PRIMARILY LOCATED IN RURAL AREAS INSIDE THE UNITED STATES. THE EVENT WAS NAMED 'SHOOTING SHERIFFS SATURDAY' AND WAS UNDERTAKEN IN RETALIATION FOR WHAT THE GROUP CONSIDERED UNJUST PROSECUTION OF 'ANONYMOUS' HACKTIVISTS.

AN ADDITIONAL 167.08KB FILE WAS RELEASED AND POSTED TO PASTEBIN AT THE FOLLOWING LOCATION: HTTPS: //PASTEBIN.COM/IKSURKUJ

RECENT FREEDOM OF INFORMATION ACT REQUESTS TURNED UP THE FOLLOWING RESPONSES FROM THESE LAW ENFORCEMENT ORGANIZATIONS:

COMMUNICATION WITH PERRY COUNTY SHERIFFS OFFICE, PERRY COUNTY, ARKANSAS:

Ms. [redacted]

We have not had any reports of hacked information from our website. I have checked with the Sheriff and our local city departments. There has not been a report of such in Perry County Arkanas.

Thank you,

Billie McCormick

C.I.D Administrative Assistant / Civil Process

Perry County Sheriff's Office

106 N. Oak St.

Perryville, AR 72126

COMMUNICATION WITH BAXTER COUNTY SHERIFFS OFFICE,BAXTER CO. ARKANSAS:

It appears this is old, from 2011 or 2012. All of that information was turned over to the FBI and you would have to contact them. We did not maintain any files

Sheriff John Montgomery

COMMUNICATION WITH IZARD COUNTY SHERIFFS OFFICE, IZARD CO., ARKANSAS:

From: Izard County Sheriff'S Office

Subject: Re: Arkansas Freedom of Information Act Request: Shooting Sheriffs Saturday (Izard County Sheriff'S Office)

We dont have and information of threats on Sheriffs

Earnie

From:

Subject: RE: Arkansas Freedom of Information Act Request: Shooting Sheriffs Saturday (Izard County Sheriff'S Office)

That's not what was requested.

From: Izard County Sheriff'S Office

Subject: Re: Arkansas Freedom of Information Act Request: Shooting Sheriffs Saturday (Izard County Sheriff'S Office)

We dont have any of these records

Earnie

From:

Subject: RE: Arkansas Freedom of Information Act Request: Shooting Sheriffs Saturday (Izard County Sheriff'S Office)

To be clear, you're asserting that your office has zero records of its being (very publicly) hacked in 2011?

From: Izard County Sheriff'S Office

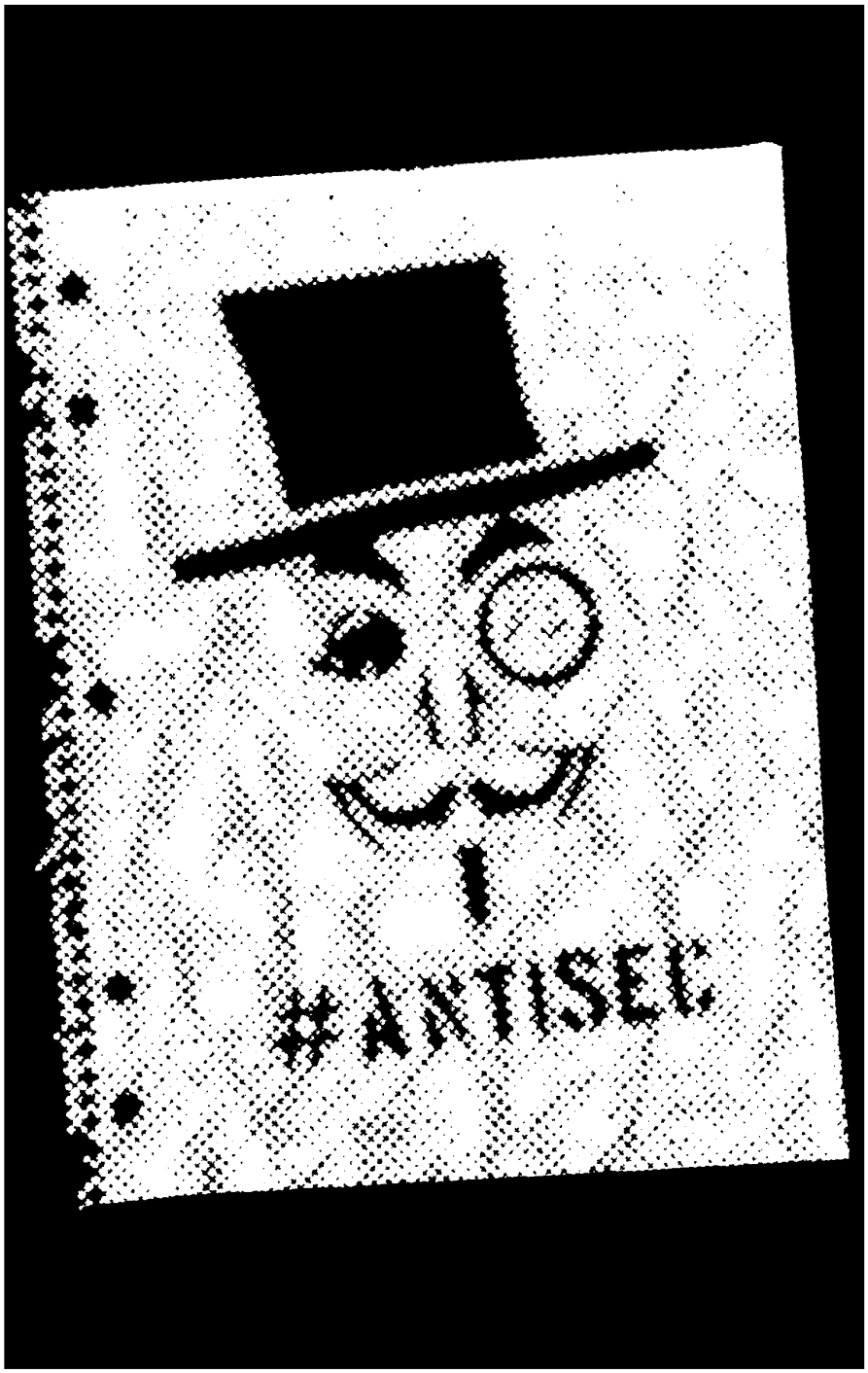
Subject: Re: Arkansas Freedom of Information Act Request: Shooting Sheriffs Saturday (Izard County Sheriff'S Office)

I was the Chief Deputy in 2011 I dont remember any reports of this
Sheriff Tate Lawrence was Sheriff then I don't remember anything. Just
talked to my now Chief Deputy that was the Chief Investigator then and
he don't remember anything either. He is the one than has a memory like
a elephant.

Earnie

CASEFILE WILL REMAIN OPEN AS ONGOING REQUESTS FOR INFORMATION (RFIS) ARE PROCESSED.

////////////////////////////////////
FOR OFFICIAL USE ONLY
SPECIAL RELEASE//SOCA
////////////////////////////////////



SEARCHED ___ INDEXED ___
SERIALIZED ___ FILED ___
☐ AT OMS ☐ SV FOIMS
☐ AT GENERAL ☐ SV GENERAL
JUL - 8 1999
FBI - ATLANTA

////////////////////////////////////
FOR PUBLIC CONSUMPTION - DECLASSIFIED
////////////////////////////////////

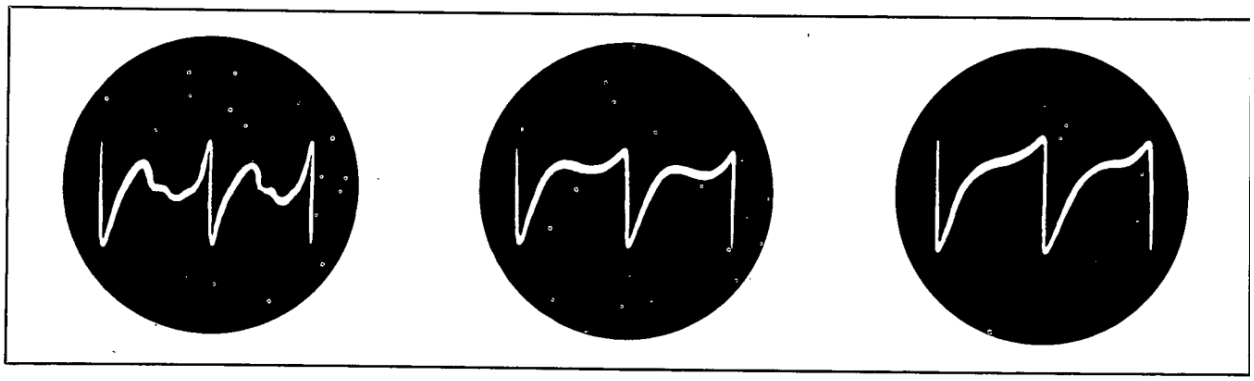


Figure A
Good 20 Microsecond Grid Pulse Shape

Figure B
Good 4 Microsecond Grid Pulse Shape

Figure C
Good 1 Microsecond Grid Pulse Shape

Figures A, B and C illustrate proper shapes of grid pulse patterns; the first hump is sufficiently high to insure a steep rise at the point of oscillation, thus keeping the time of plate current flow just before oscillation to a minimum. The hump itself is well below the level at which it would cause the tube to draw plate current.

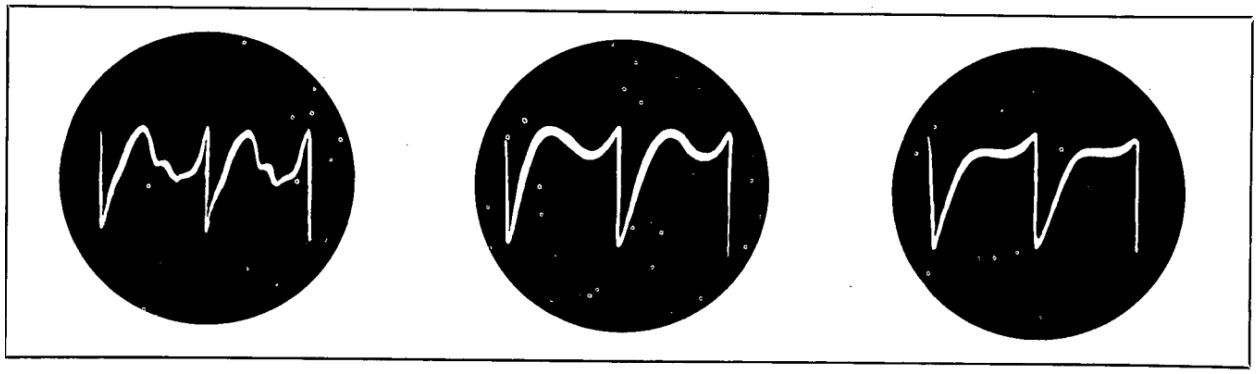
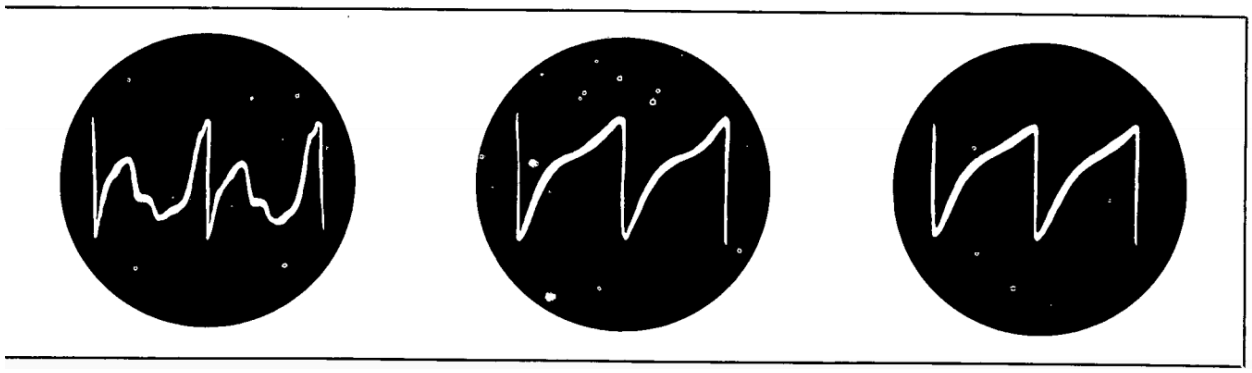


Figure D
Poor 20 Microsecond Grid Pulse Shape

Figure E
Poor 4 Microsecond Grid Pulse Shape

Figure F
Poor 1 Microsecond Grid Pulse Shape

Figures D, E and F illustrate grid pulse shapes in which the hump is too high and is causing plate current to flow at the top. If the hump were to go still higher, it would rise above the level at which the tube oscillates resulting in "multiple pulsing" and erratic patterns on both the grid pulse viewing scope and the indicator scopes.



////////////////////////////////////
FOR PUBLIC CONSUMPTION - DECLASSIFIED
////////////////////////////////////

== ==

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION ARCHIVAL RECORDS

== ==

DRAFTED BY: Teletypist

PARTNER AGENCY, NATIONAL AERONAUTICS AND SPACE ADMINISTRATION (NASA) REPORTS THAT A BREACH OF THE SPACE PHYSICS ANALYSIS NETWORK (SPAN) HAS TAKEN PLACE AND RESULTED IN A "WORM" BEING RELEASED INTO THE AGENCY'S PRIMARY ANALYTIC NETWORK.

```
 W O R M S   A G A I N S T   N U C L E A R   K I L L E R S
_____________________________________________________________
\__  ____________  _____    ________    ____  ____   __  _____/
 \ \ \    /\    / /    / /\ \       | \ \  | |    | | / /    /
  \ \ \  /  \  / /    / /__\ \      | |\ \ | |    | |/ /    /
   \ \ \/ /\ \/ /    / ______ \     | | \ \| |    | |\ \   /
    \_\  /__\  /____/ /______\ \____| |__\ | |____| |_\ \_/
     \____________________________________________________/
      \                                                   /
       \    Your System Has Been Officially WANKed      /
        \_____________________________________________/

You talk of times of peace for all, and then prepare for war.
```

INTERNAL REPORTING ON THE INCIDENT WHICH TOOK PLACE IN 1989 APPEARS AS FOLLOWS:

NASA
National Aeronautics and
Space Administration

GMSR Report

November 1989

NASA
OFFICE OF MANAGEMENT

INFORMATION RESOURCES MANAGEMENT

SPACE PHYSICS ANALYSIS NETWORK (SPAN) WORM INCIDENT

BACKGROUND ON SPAN

- CREATED IN 1981 FOR OPEN EXCHANGE OF SCIENTIFIC INFORMATION BY RESEARCHERS
- COMPOSED OF INTERNATIONAL NETWORK OF APPROXIMATELY 6,000 NODES SERVING APPROXIMATELY 100,000 USERS:
  - GOVERNMENT (APPROXIMATELY 600 NASA MANAGED)
  - PRIVATE INDUSTRY
  - UNIVERSITY
- CAN BE ACCESSED FROM ALMOST ANYWHERE IN WORLD USING A PERSONAL COMPUTER AND TELEPHONE

NASA
OFFICE OF MANAGEMENT

INFORMATION RESOURCES MANAGEMENT

SPACE PHYSICS ANALYSIS NETWORK (SPAN) WORM INCIDENT

DESCRIPTION OF ATTACK

- ORIGIN TRACED TO FRANCE
- WORM CODE:
  - EXPLOITS POOR PASSWORD MANAGEMENT PRACTICES
    - NASA VICTIMS FAILED TO FOLLOW PUBLISHED AGENCY POLICIES AND PROCEDURES
  - CAUSES
    - DISRUPTION AND DENIAL OF SERVICE
    - EXPENDITURE OF RESOURCES TO TECHNICALLY DIAGNOSE AND DISINFECT AFFECTED SYSTEMS
    - DISPLAY OF BANNER ON USER SCREENS
- TWO PHASED ATTACK
  - OCT 16 ATTACK AFFECTED APPROXIMATELY 90 NODES
  - OCT 29 ATTACK AFFECTED OVER 500 NODES
    - USED IMPROVED VERSION TO EXPLOIT ADDITIONAL PASSWORDS
- SPECIFIC IDENTIFICATION OF PENETRATED NODES UNDERWAY
  - ONLY 3 IDENTIFIED AT NASA TO DATE
- ATTACK IS STILL ACTIVE

NASA
OFFICE OF MANAGEMENT

INFORMATION RESOURCES MANAGEMENT

SPACE PHYSICS ANALYSIS NETWORK (SPAN) WORM INCIDENT

EFFORTS TO REDUCE FUTURE RISK EXPOSURE

- INSTRUCTIONS BEING REISSUED TO ALL NODE MANAGERS TO STRENGTHEN PASSWORD MANAGEMENT PRACTICES
- SELECTED NETWORK NODES (NASA AND NON-NASA) WILL BE AUDITED TO ASSURE COMPLIANCE WITH PASSWORD MANAGEMENT INSTRUCTIONS
- NASA/IG AND FBI ARE INVESTIGATING FOR PROSECUTION

HOWEVER

- OPEN INTERNATIONAL NETWORKS WILL ALWAYS HAVE A CERTAIN LEVEL OF VULNERABILITY

INTERNAL REPORTING IS CONSISTENT WITH WHAT HAS BEEN ACCEPTED AS THE PUBLIC NARRATIVE AROUND THE SPAN BREACH OF 1989.

IT IS ALSO POSSIBLE THAT WANK HAD MULTIPLE VARIANTS,ALTHOUGH THIS INFORMATION HAS NOT YET BEEN VERIFIED BY INTERNAL NASA REPORTING.

Blessed Be The Mother

OFFICE OF INTERNAL ASSET RECOVERY

////////////////////////////////////
FOR OFFICIAL USE ONLY
SPECIAL RELEASE//SOCA
////////////////////////////////////

APPROVED BY: DAULTON, JACK, [redacted] B7E

DRAFTED BY: Teletypist

CASE ID #: A224-AT-45839

TITLE: "HELLO? IS IT W3AF YOURE LOOKING FOR?"
ANTISEC
AGENT [redacted] - VICTIM B7E
GOOGLE INC - VICTIM
INTRUSION - INFO SYSTEMS
IDENTITY THEFT
CONSPIRACY
CRIMINAL HARASSMENT

KEY JUDGEMENTS:

Φ FBI AGENTS WERE TARGETED BY ANTISEC ACTORS WHO EXPLOITED GOOGLE ACCOUNTS TO SEND TEXT MESSAGES TO AGENT TELEPHONES.

Φ IMPORTANT TOOLS TECHNIQUES AND PROCEDURES EXPOSED IN THE PROCESS OF AN ONGOING CAMPAIGN OF AGENT HARASSMENT

ACCORDING TO TESTIMONY PROVIDED BY BUREAU PERSONNEL, A RENOWNED HACKING GROUP KNOWN AS ANTISEC HAS SUCCESSFULLY EXPLOITED GOOGLE ACCOUNTS USED BY FBI AGENTS.

--- TEAR LINE - INTERNAL RECORDS - TEAR LINE ---

ACCORDING TO INTERNAL TESTIMONY,THE ACCOUNTS WERE BREACHED PRIOR TO 2011 AND USED AS PART OF AN INTIMIDATION CAMPAIGN AGAINST THE AGENT IN QUESTION:

Details: On 11/18/2011, retired California Department of Justice Special Agent Supervisor [redacted] advised that he received text messages from his own Google telephone number indicating that he had been "owned".

On 11/18/2011, at approximately 7:00 am PST, [redacted] began receiving text messages on his cellular telephone from the telephone number associated with his Google Voice account, [redacted] The text messages were statements similar to "We have you" and "We own you". Additional text messages were received that directed [redacted] to enter an IRC chat room to discuss the matter with the individuals that had taken over [redacted] accounts. [redacted] advised that he did not reply to these messages and does not recall the exact context of the messages or the name of the IRC chat room that they were directing him to. [redacted] stated that he has deleted the text messages and has no record of them.

b6
b7C

Shortly after receiving the text messages from the individuals claiming they had compromised his accounts, [redacted] began receiving telephone calls from friends and family members who advised him that they were receiving suspicious messages from him on Facebook. The individuals also advised that there were [redacted] and other out of character posts on his Facebook feed.

THE CAMPAIGN DID NOT STOP WITH TELEPHONIC HARASSMENT. THE ACTORS THEN CONTINUED OPERATIONS AGAINST THE AGENT IN QUESTION:

By noon [redacted] had recovered and locked down all of his accounts. Text messages continued arriving on his cellular telephone that appeared to be from his Google Voice telephone number. Fearing that his Google account was still compromised, [redacted] deleted the Google account.

b6
b7C

Following the recovery of his accounts, [redacted] received a text message that stated that it wasn't over and a text message that made a reference to the tough economic times and financial

issues. [redacted] checked his credit cards and discovered that a fraudulent charge had been made on his [redacted] card from Ritz camera. The item was set to ship to his old address. The [redacted] card that was used ended in [redacted] b6 b7C

[redacted] believed that the compromise could be related to his Android cellular telephone, which he had "rooted". One of the consequences of rooting the telephone was that other programs that normally would not have access to the files "Shared Preferences" and "Accounts.db" could now access those files. The files contain information such as [redacted] from the telephone. A few days prior to the individuals advising [redacted] that he had been compromised [redacted] had downloaded and installed a program called "atorrent" from the Android store. This program allowed a user to download torrent files onto your cellular telephone. [redacted] stated that he used the program several times to test it, downloading music and a movie. b6 b7C

[redacted] also stated that his laptop could have been a potential source of the compromise, but did not believe that it could have been his desktop computer.

IN THIS PIECE OF TESTIMONY,A PIECE OF THE TOOLS TECHNIQUES AND PROCEDURES (TTP) ARE EXPOSED SHOWING HOW THE ACTORS WERE ABLE TO CONDUCT THEIR OPERATIONS AGAINST THE VICTIMS MOBILE PHONE. THE VICTIMS MOBILE PHONE WAS COMPROMISED AND ADDITIONAL TOOLS WERE ABLE TO BE DOWNLOADED TO THE DEVICE VIA A TORRENT-BASED MOBILE APPLICATION.

POSSIBLE AVENUE OF INFECTION FOR THE AFOREMENTIONED MOBILE DEVICE MAY HAVE BEEN AN ASSOCIATED PERSONAL COMPUTER.

Well Would You Look At That!

The Federal Bureau of Investigation (FBI) has claimed to have no documentary knowledge of w00w00 between the years of 1996 and 2010 and has affirmed their lack of responsive docs after appeal. *Fascinating*!

U.S. Department of Justice
Office of Information Policy
Suite 11050
1425 New York Avenue, NW
Washington, DC 20530-0001

Telephone: (202) 514-3642

Re: Appeal No. DOJ-AP-2019-005003
Request No. 1435292
CDT:DRC

VIA: Email

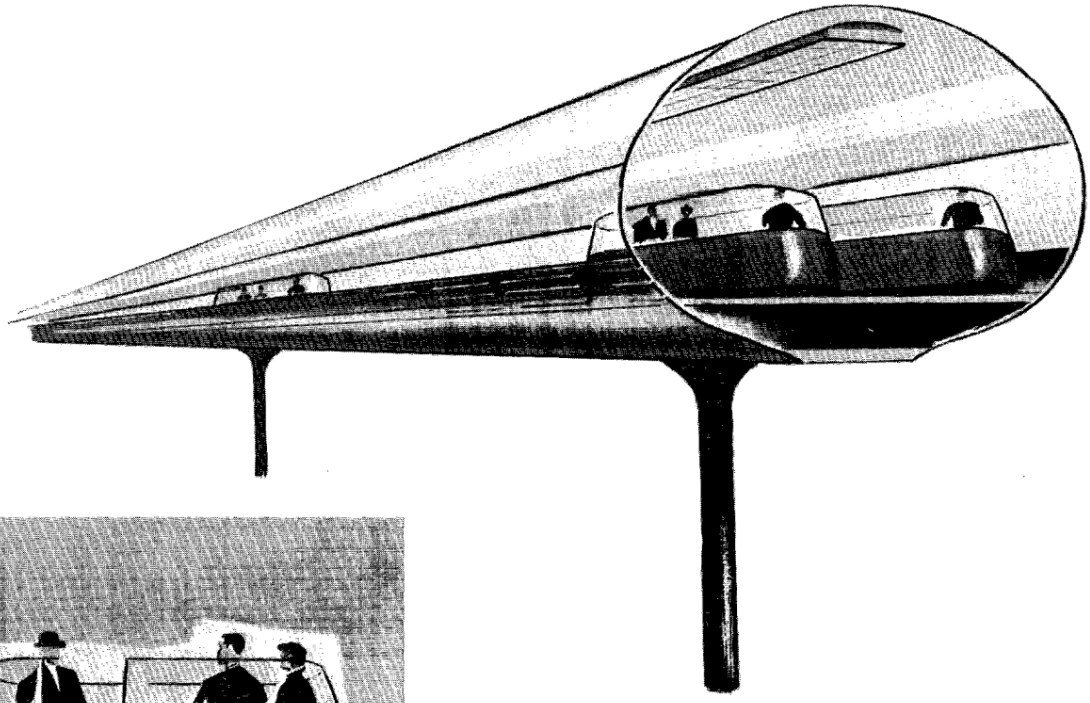
You appealed from the action of the Federal Bureau of Investigation on your Freedom of Information Act request for access to records concerning w00w00 Hacking Group from 1996 to 2010. I note that you have appealed the adequacy of the FBI's search for responsive records. Please note that this Office was closed due to a lapse in funding appropriations between December 22, 2018 and January 25, 2019, which resulted in a delay in responding to your appeal.

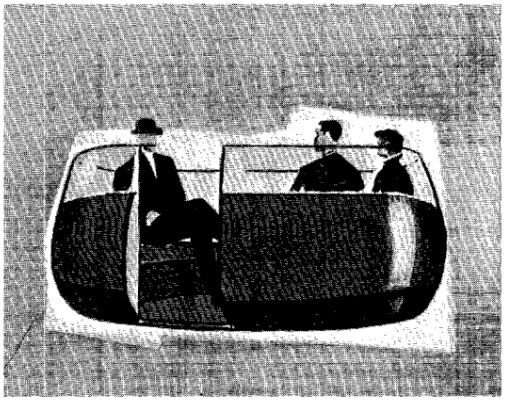
After carefully considering your appeal, I am affirming the FBI's action on your request. The FBI informed you that it could locate no responsive records subject to the FOIA in its files. Please be advised that the FBI searched its automated indices and Sentinel database and located no responsive records, searching using both numeric "0" characters and alphabetic "O" characters. I have determined that the FBI's action was correct and that it conducted an adequate, reasonable search for such records.

CARVEYOR

PASSENGER CONVEYOR SYSTEM

CONTINUOUS SERVICE, NO-WAITING
MINI-TRANSPORTATION SYSTEM





TRANSPORTATION FOR THE 1970's

- Airport Terminals
- Central Business Districts
- Major Activity Centers
- Special Purpose Applications

//////////////////////////////////////
DECLASSIFIED - CENTRAL INTELLIGENCE AGENCY ARCHIVE
//////////////////////////////////////

OFFICE OF INTERNAL ASSET RECOVERY
TOOL INVESTIGATION

////////////////////////////////////
UNCLAS FOR OFFICIAL USE ONLY//PIZZATIME
////////////////////////////////////

APPROVED BY:DAULTON,JACK, B7E

DRAFTED BY: Teletypist

KEY BACKGROUND:

Φ BACK ORIFICE IS A TOOL CREATED BY A GROUP KNOWN AS 'CULT OF THE DEAD COW'

Φ THIS TOOL HAS BEEN RELEASED TO THE PUBLIC AND APPEARS TO HAVE BEEN USED IN THE PURSUIT OF RECENT NETWORK INTRUSIONS.

TITLE: UNSUB;
VEGETABLE, DETH;
NINJA,NET;
CULT OF THE DEAD COW
"BACK ORIFICE"

THE FOLLOWING IS A SET OF MEMORANDUM SUMMARIES ON THE CREATION, CAPABILITIES AND RELEASE OF THE TOOL REFERRED TO IN PUBLIC REPORTING AS QUOTE BACK ORIFICE UNQUOTE (OR SOMETIMES REFERRED TO IN THESE DOCUMENTS AS 'BO').

IN DOCUMENTS DATED Ø7/22/1999 BACK ORIFICE IS DISCUSSED WITHIN;

APPROPRIATE DOD FACILITIES, SERVICE COMPONENTS AND TARGET LOCATIONS; [redacted]

b7E

SUBJECT: [redacted]

GROUP IN EXISTENCE SINCE 1984) RELEASED A PRODUCT CALLED QUOTE BACK ORIFICE UNQUOTE AT LAST YEAR'S DEFCON VI HACKER CONVENTION. CDC HAS ANNOUNCED PLANS TO RELEASE A NEW VERSION OF BACK ORIFICE (BACK ORIFICE 2000) ON JULY 10TH AT THE DEFCON VII CONVENTION LAS VEGAS. THE PRODUCT WILL BE MADE AVAILABLE AS A FREE DOWNLOAD ON THAT DATE.

2. (U) THE ORIGINAL 1998 RELEASE OF BACK ORIFICE INCLUDED THE FOLLOWING CAPABILITIES:

A. RETRIEVAL OF SYSTEM INFORMATION INCLUDING CURRENT USER, CPU TYPE, WINDOWS VERSION, MEMORY USAGE, MOUNTED DISKS AND DRIVE INFORMATION, SCREENSAVER PASSWORD, AND PASSWORDS CACHED BY USERS (DIAL-UPS, WEB AND NETWORK ACCESS, ETC).

B. FILE SYSTEM CONTROL: COPY, RENAME, DELETE, VIEW, SEARCH,

COMPRESS, AND DECOMPRESS FILES.

C. PROCESS CONTROL: LIST, SPAWN, KILL.

D. REGISTRY CONTROL: LIST, CREATE, DELETE, SET KEYS AND VALUES.

E. NETWORK CONTROL.

F. MULTIMEDIA CONTROL (INCLUDING SCREEN CAPTURE).

G. PACKET REDIRECTION AND SNIFFING.

H. APPLICATION REDIRECTION (SPAWN MOST APPLICATIONS ON A SPECIFIC PORT, SUCH AS TELNET).

I. HTTP SERVER (UPLOAD AND DOWNLOAD FILES).

J. RUNS ON START-UP WITH NO ENTRY IN THE TASK LIST.

3. (U) BACK ORIFICE 2000 WILL REPORTEDLY INCLUDE SEVERAL FEATURES NOT FOUND IN THE ORIGINAL VERSION, INCLUDING WINDOWS NT COMPATIBILITY (THE ORIGINAL PROGRAM ONLY WORKED ON WINDOWS '95/98), OPEN PLUG-IN ARCHITECTURE FOR 3RD PARTY ADD-ONS, STRONG CRYPTOGRAPHY, AND OPEN SOURCE CODE AVAILABLE UNDER GNU PUBLIC LICENSE.

4. (U) ASSESSMENT.

A. (FOUO) BACK ORIFICE 2000 WINDOWS NT COMPATIBILITY COULD

BT

#0063

TEXT CONTINUES:

GREATLY INCREASE THE POTENTIAL FOR DAMAGE TO NETWORK INFRASTRUCTURE. THE PREVIOUS VERSION ONLY AFFECTED WINDOWS 95/98 MACHINES, GENERALLY USED AS NETWORK CLIENTS. HOWEVER, INFECTION OF NETWORK SERVERS (COMMONLY RUNNING WINDOWS NT) COULD DRAMATICALLY INCREASE THE POTENTIAL IMPACT OF AN INFECTION IN TERMS OF BOTH DATA LOSS AND CONNECTIVITY DISRUPTION.

B. (FOUO) THE EXPECTED COMBINATION OF OPEN SOURCE CODE AND PLUG-IN ARCHITECTURE WOULD MAKE BACK ORIFICE 2000 POTENTIALLY MORE DESTRUCTIVE AND DIFFICULT TO ERADICATE THAN ITS PREDECESSOR. THE ORIGINAL BACK ORIFICE WAS FOLLOWED BY A SMALL NUMBER OF THIRD-PARTY ADD-ONS; IT APPEARS THAT CDC IS MAKING AN EFFORT TO ENCOURAGE THIRD-PARTIES TO ENHANCE BACK ORIFICE 2000, IN LINE

WITH THE GENERAL PHILOSOPHY OF OPEN-SOURCE PROGRAMMING ADVOCATES. EXPECT SIGNIFICANT VARIANTS TO APPEAR AFTER THE INITIAL RELEASE WHICH COULD INCLUDE VARIOUS PROPAGATION FEATURES, REMOTE INFORMATION TRANSMISSION, OR CORRUPTION AND DESTRUCTION OF DATA. THESE VARIANTS MAY REQUIRE ANTI-VIRUS SOFTWARE AND NETWORK PROTECTION UPDATES. EXPECTED BACK ORIFICE 2000 FEATURES COULD EASILY INCORPORATE CUSTOMIZED MALICIOUS CODE WITH THE BASIC PRODUCT.

5. ~~(FOUO)~~ RECOMMENDATIONS. BACK ORIFICE 2000 WILL LIKELY BE USED IN A SELECTIVE OR TARGETED MANNER SIMILAR TO PREVIOUS NETWORK SECURITY EXPLOITS. EXPECTED NT COMPATIBILITY WILL MAKE CORPORATE, GOVERNMENT, AND MILITARY SYSTEMS INCREASINGLY ATTRACTIVE TARGETS. THESE COMMONLY TARGETED GROUPS SHOULD AGGRESSIVELY REVIEW AND MONITOR COMPREHENSIVE SECURITY MEASURES TO PROTECT AGAINST THE KIND OF EXPLOITS CAUSED OR SUPPORTED BY BACK ORIFICE 2000. ADDITIONALLY, SUBSEQUENT MODIFICATION OF BACK ORIFICE 2000 FOR EXPANDED MALICIOUS IMPACT IS POSSIBLE, AND SHOULD BE IMMEDIATELY REPORTED.

Reader's Note: the storied history of Back Orifice is recorded here in a clinical format by the original FBI analyst. Notable in the analysis of this tool is how the FBI characterized its possible impact on corporate, government, and military systems. Also noteworthy is the grasp that the analyst has over the contemporary value of BO at the time of its release.

'Letter From The Editor'

Dear Reader,

It has been my greatest privilege to prepare this publication for you all to be able to appreciate The Freedom of Information Act (FOIA). FOIA has been an incredible tool for legal government transparency. A tool that promises a future for citizen control over their public servants.

However, FOIA is a tool that requires care and feeding. It was Emma Goldman who said, "People have only as much liberty as they have the intelligence to want and the courage to take." We have been given a wonderful tool by those giants whose shoulders we stand on today, and it is up to us to preserve and expand the strength of this tool in the face of coercion and despotism.

Freedom and decency are the twin blessings of a healthy republic and we who are here today bear the obligation to maintain both.

The history of hacking and hackers is a story of curiosity, with a healthy dose of anarchy. It is an important history, and it is *our* history. Many of us would not be here were we not representatives of chaos in one form or another. We are all cut from the same cloth, with many of the same broad virtues.

We value openness, compassion, thoughtfulness, and it is in that spirit that we all must treat each other with reverence, respect, and most of all, love. These past 5 years have been tough and have shown artificial divisions in our connections to one another.

Although these are hard times, when we come together, we have to remember our shared history. We are all oddballs and screw-ups, outcasts and introverts. Indeed, some of us even have crimes in our past.

My solemn as we remember this shared history is that we will rediscover the love we all once had for each other as misfit children just trying to survive in this fucked up, madcap world.

Yours Truly,

Sister Eliza Concordia <3

With Special Thanks To:

Sister Emma Best – For their punctuality, and blessed skills in governmental intimidation & vexation.

Sister Sarah Allen Reed (sarahallenreed.com) – For her ethereal illustrations & impeccable taste.

--- Tear Line ---

If you have any compliments, encouragements, or otherwise forms of praise, please do not hesitate to reach out to our trusted agent on twitter: @hexadecim8.

If you would like to submit culture to a future edition of The Teletypist, please contact @hexadecim8.

For any concerns, complaints, or unspecific forms of harassment, please contact /dev/null